InfoGuard
SWISS CYBER SECURITY

Checklist

Protection against Social Engineering

Cyberattacks today no longer target only technology but increasingly focus on people. In so-called social engineering attacks, perpetrators deliberately manipulate employees in order to obtain confidential information or gain access to systems.

Companies invest in modern security solutions and technical safeguards, but even the best technology cannot prevent sensitive data from being disclosed through human behaviour.

This is precisely where social engineering attacks come into play. It is therefore all the more important to raise awareness among yourself and your employees and to define clear behavioural guidelines. The following practical tips will help you identify social engineering attacks at an early stage and protect yourself effectively against them.

15 Practical tips for protection against social engineering in everyday business

1. Do not disclose any confidential information (whether by email, telephone or on social media) and avoid discussing business matters in public.
2. Store confidential information securely, lock your computer when leaving your workplace, and shred documents that are no longer needed.
3. Approach unknown visitors if they are moving around company premises unaccompanied. Verify their information if in doubt.
4. Do not connect unknown USB sticks to your computer.
5. Only publish as much information as necessary on the internet and social networks.
6. Only accept friend requests on social media from people you genuinely know. If in doubt, verify first.
7. Never share personal passwords and use different passwords with at least 12 characters, including letters, numbers and special characters.
8. Prevent others from seeing your password when entering it – just as you would at an ATM.
9. Do not simply dismiss security warnings and notifications! They contain important information. If unsure, contact your helpdesk.
10. Disable macros in Office programs such as Word, Excel and PowerPoint, as they may contain malicious code.
11. Do not open suspicious emails and check the sender's address carefully. Report such emails immediately to your IT department.
12. If you have accidentally opened a suspicious email:
    a. Do not open attachments or click on links – even if explicitly requested.
    b. Check whether a sense of urgency is being created (e.g. "act now!" or "urgent!") or if you are being asked to provide sensitive data.
    c. Pay attention to how it addresses you.
13. Verify links in emails by hovering over them – does the displayed link match the actual destination?
14. Stay informed about current threats, as cybercriminals are using increasingly credible methods in the age of AI (e.g. deepfakes and voice cloning), making attacks more convincing and scalable.
15. Read internal security and data protection policies carefully and follow the established processes.

Your Cybersecurity – Our Passion & Expertise

Cyber Defence & Incident Response are essential, but only two aspects of comprehensive and effective cybersecurity. Our 360° cyber security approach also includes Cloud Security, Managed Security & Network Solutions for IT, OT and cloud infrastructures, Penetration Testing & Red Teaming, as well as Security Consulting Services. Our SOC services are delivered from our ISO 27001-certified and ISAE 3000 Type 2 audited Cyber Defence Center (CDC) in Switzerland and Germany – with 24/7 operations and continuous staffing.

We are happy to support you in protecting yourself against Social Engineering

Contact us for a no-obligation consultation.

info@infoguard.ch · www.infoguard.ch

Baar (Head Office)
InfoGuard AG
Lindenstrasse 10
6340 Baar
Switzerland
infoguard.ch

Bern
InfoGuard AG
Stauffacherstrasse 141
3014 Bern
Switzerland
infoguard.ch

Frankfurt
InfoGuard Deutschland GmbH
Frankfurter Straße 233
63263 Neu-Isenburg
Germany
infoguard.de

Munich
InfoGuard Deutschland GmbH
Landsberger Straße 302
80687 Munich
Germany
infoguard.de

Düsseldorf
InfoGuard Deutschland GmbH
Am Gierath 20A
40885 Ratingen
Germany
infoguard.de

Vienna
InfoGuard GmbH
Kohlmarkt 8-10
1010 Vienna
Austria
infoguard.at